CLAIMS

What is claimed is:

1. A method, comprising:

loading a virtual machine monitor (VMM) to support a service virtual machine (VM) and a guest VM of a computer system;

invoking a service operating system (OS) in the service VM during the pre-boot phase of the computer system, the service OS to allow observation of a guest OS;

invoking the guest OS in the guest VM; and

switching between the guest VM and the service VM during an OS runtime of the guest OS.

2. The method of claim 1 wherein the VMM to operate in accordance with instructions stored in a non-volatile storage device of the computer system.

3. The method of claim 1, further comprising switching from the guest VM to the service VM in response to a trap event, wherein the trap event includes detecting a violation of a policy of the computer system by the VMM.

4. The method of claim 3, further comprising setting the policy of the trap event during the pre-boot phase of the computer system.

5. The method of claim 1, further comprising:

periodically checking for a fault condition of the guest OS by the VMM; and

switching to the service VM if the VMM detects the fault condition.

6. The method of claim 1, further comprising switching to the service VM from the guest VM in response to a user request.

7. The method of claim 1, further comprising unloading the VMM and executing the guest OS in a non-virtual machine environment of the computer system.

8. The method of claim 1 wherein the VMM is loaded during the pre-boot phase of the computer system.

9. The method of claim 1 wherein invoking the guest OS is initiated by a switch from the service VM.

10. The method of claim 1 wherein switching between the guest VM and the service VM is completed without rebooting the computer system.

11. The method of claim 1 wherein switching between the guest VM and the service VM is performed by firmware of the computer system.

12. The method of claim 1 wherein operations of the VMM are assisted by microcode of a processor of the computer system.

13. An article of manufacture comprising:

a machine-readable medium including a plurality of instructions which when executed perform operations comprising:

loading a virtual machine monitor (VMM) during a pre-boot phase of a computer system, the VMM to support a service virtual machine (VM) and a guest VM of the computer system;

booting a service operating system (OS) during a pre-boot phase of a computer system into the service VM, wherein the service OS to provide tools to diagnose a guest operating system of a computer system;

booting the guest OS into the guest VM to begin a guest OS runtime of the computer system; and

performing a VM switch between the guest VM and the service VM during the guest OS runtime without rebooting the computer system.

14. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising performing the VM switch from the service VM to initiate the booting of the guest OS.

15. The article of manufacture claim 13 wherein the VMM to operate in accordance with an Extensible Firmware Interface (EFI) framework standard.

16. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising:

establishing a trap event of the computer system, wherein the trap event includes detecting a violation of a policy of the computer system by the VMM; and

performing the VM switch from the guest VM to the service VM in response to detecting the trap event.

17. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising

establishing a polling event of the computer system, wherein the polling event includes periodically checking for a fault condition of the guest OS by the VMM; and

performing the VM switch from the guest VM to the service VM in response to detecting the fault condition of the guest OS during the polling event.

18. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising performing the VM switch from the guest VM to the service VM in response to a user request to perform the VM switch.

19. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising unloading the VMM and executing the guest OS in a non-virtual machine environment of the computer system.

20. The article of manufacture of claim 13 wherein the VM switch is performed by firmware of the computer system.

21. The article of manufacture of claim 13 wherein the VM switch is assisted by microcode of a processor of the computer system.

22. A computer system, comprising:

a processor; and

at least one flash device operatively coupled to the processor, the at least one flash device including firmware instructions which when executed by the processor perform operations comprising:

loading a virtual machine monitor (VMM) on the computer system during a pre-boot phase of the computer system;

booting a service operating system (OS) in a service virtual machine (VM) during the pre-boot phase, the service OS to enable analysis of the computer system;

booting a guest OS in a guest VM of the computer system in response to a VM switch from the service OS to the service OS; and

performing the VM switch from the guest VM to the service VM during an OS runtime of the guest OS in response to a fault of the guest OS.

23. The computer system of claim 22 wherein the fault of the guest OS comprises violation of a policy setting of the computer system.

24. The computer system of claim 23 wherein execution of the plurality of instructions further perform operations comprising generating a user interface during the pre-boot phase to receive the policy setting to trigger the VM switch during the OS runtime of the guest OS.

25. The computer system of claim 22 wherein the fault is detected during a periodic computer system check by the VMM to determine a status of the guest OS.

26. The computer system of claim 22 wherein execution of the plurality of instructions further perform operations comprising performing the VM switch in response to a user request.

27. The computer system of claim 22 wherein the VM switch to occur without re-booting the computer system.

28. The computer system of claim 22 wherein the processor includes microcode to assist operations of the VMM.

29. The computer system of claim 22 wherein the firmware to operate in accordance with an Extensible Firmware Interface (EFI) framework standard.